WHAT IS CLAIMED IS:

1. A content management method for a data storage provided with a plurality of content storing means, comprising the steps of:

decrypting, with a first storage key, a content key encrypted with the first storage key and stored along with a content encrypted with the content key in a first content storing means;

encrypting the content key obtained by the above decryption with a newly generated second storage key; and

storing the content key encrypted with the second storage key along with the encrypted content in a second content storing means.

2. The method as set forth in Claim 1, wherein the second storage key is generated based on a random number.

3. The method as set forth in Claim 1, wherein the content key obtained by the decryption is encrypted with identification information of the second content storing means and stored into the second content storing means.

4. The method as set forth in Claim 1, wherein the content key is encrypted, in the first content storing means, with the first storage key and identification information of the first content storing means, and the content key stored in the first content storing means is decrypted with the first storage key and identification information of the first content storing means.

5. The method as set forth in Claim 1, wherein the second storage key is

generated by a decrypted key generating means provided in the data storage.

6. The method as set forth in Claim 5, wherein the second storage key is encrypted with a public key for a key management unit for management of the storage keys to generate a third storage key and the third storage key is stored into the second content storing means.

7. The method as set forth in Claim 6, wherein the data storage deletes the second storage key depending upon whether the third storage key has been stored in the second content storing means.

8. The method as set forth in Claim 7, wherein when decrypting the content key stored in the second content storing means, the data storage sends the third storage key to the key management unit; and the key management unit generates a second storage key based on the third storage key while accounting the data service following a predetermined procedure.

9. The method as set forth in Claim 1, wherein the second storage key is generated by a storage key generating means provided in the key management unit which manages the storage keys; and the key management unit has stored therein the second storage key and the identification information of the second content storing means in which the content key encrypted with the above generated second storage key.

10. The method as set forth in Claim 9, wherein upon the generation of the second storage key, the key management unit accounts the data service following

the predetermined procedure.

11. The method as set forth in Claim 9, wherein the key management unit encrypts the second storage key with the management key to generate a third storage key, and sends the third storage key to the data storage; and the data storage stores the received third storage key into the second content storing means.

12. The method as set forth in Claim 11, wherein the data storage deletes the second storage key depending upon whether the third storage key has been stored in the second content storing means.

13. The method as set forth in Claim 12, wherein the key management unit has stored therein the identification information of the second content storing means in which the content key encrypted with the second storage key; the data storage sends, when decrypting the content key stored in the second content storing means, the identification information of the second content storing means to the key management unit; and the key management unit generates a second storage key based on the result of comparison between the identification information of the second content storing means, send from the data storage, and the identification information of the second content storing means, held in the key management unit itself, while accounting the data service following the predetermined procedure.

14. The method as set forth in Claim 1, wherein the second content storing means has stored therein the identification information of the data storage.

15. The method as set forth in Claim 14, wherein the data storage starts decrypting the content key stored in the second content storing means depending upon the result of an inspection of the identification information of the data storage, stored in the second content storing means.

16. The method as set forth in Claim 1, wherein the decrypted content key supplied from the second content storing means has added thereto information that the content key is a one obtained by restoration.

17. The method as set forth in Claim 16, wherein when moving the content key having added thereto the information that the content key is a restored one, the data storage makes an error process based on the result of comparison between the content key and a content key stored in a destination to which the content key is to be moved.

18. The method as set forth in Claim 1, wherein the content key has added thereto frequency information which limits the number of times the content key can be used.

19. The method as set forth in Claim 1, wherein the content key stored in the first content storing means is stored along with the identification information of the first content storing means into the second content storing means; the identification information stored in the second content storing means is stored into the data storage when the content key stored in the second content storing means is decrypted; and the data storage makes, when a request is made to decrypt the

content key in the first content storing means, an error process based on the result of comparison between the identification information of the first content storing means in consideration and the identification information of the second content storing means.

20. A content storage system, comprising:

a first content storing means having stored therein a content key encrypted with a first storage key and a content encrypted with the content key;

means for decrypting a data and key data;

means for encrypting the data and key data;

means for generating a storage key;

a second content storing means for storing an encrypted content key obtained by encrypting, in the encrypting means, the content key obtained by decryption with the first storage key in the decrypting means, using the second storage key generated by the storage key generating means, and the encrypted content; and

means for storing the storage keys.

21. The system as set forth in Claim 20, wherein the storage key storing means generates the second storage key by means of a random number generator.

22. The system as set forth in Claim 20, wherein a content key obtained by encrypting, in the encrypting means, the content key obtained by the decryption in the decrypting means, with the first storage key and identification information of

the second content storing means, is stored in the second content storing means.

23. The system as set forth in Claim 20, wherein the content key is encrypted, in the first content storing means, with the first storage key and identification information of the first content storing means; and the content key stored in the first content storing means is decrypted with the first storage key and identification information of the first content storing means.

24. The system as set forth in Claim 20, wherein the first content storing means, decrypting means, encrypting means, second content storing means, storage key storing means and storage key generating means form together a data storage; and further comprising a key management unit which manages the storage keys of the data storage.

25. The system as set forth in Claim 24, wherein the data storage is a data receiver which receives a content encrypted and sent from a data transmitter.

26. The system as set forth in Claim 24, further comprising means for storing the public key of the key management unit; and wherein the second content storing means has stored therein the second storage key along with a third storage key obtained by encrypting the second storage key with the public key.

27. The system as set forth in Claim 26, wherein the data storage deletes the second storage key depending upon whether the third storage key is stored in the second content storing means.

28. The system as set forth in Claim 27, wherein when decrypting the content

key stored in the second content storing means, the data storage sends the third storage key to the key management unit; and the key management unit sends a second storage key generated based on the third storage key to the data transmitter while accounting the data service following a predetermined procedure.

29. The system as set forth in Claim 24, wherein the second content storing means has stored therein the identification information of the data storage.

30. The system as set forth in Claim 29, wherein the data storage starts decrypting the content key stored in the second content storing means depending on the result of inspection of the identification information of the data storage, stored in the second content storing means.

31. The system as set forth in Claim 20, wherein the first content storing means, decrypting means, encrypting means, second content storing means and storage key storing means form together a data storage; and comprising the storage key generating means and further a key management unit which manages the storage keys of the data storage.

32. The system as set forth in Claim 31, wherein the data storage is a data receiver which receives a content encrypted and sent from a data transmitter.

33. The system as set forth in Claim 31, wherein the key management unit comprises an identification information storing means in which the storage key generated by the key management unit and the identification information of the content storing means in which the content key encrypted with the generated

storage key.

34. The system as set forth in Claim 31, wherein the key management unit accounts the data service following the predetermined procedure depending upon the generation of the storage key.

35. The system as set forth in Claim 31, wherein the key management unit comprises means for storing storage keys; the key management unit generates a third storage key by decrypting the second storage key with the storage key and sends it to the data storage; and the data storage stores the third storage key into the second content storing means.

36. The system as set forth in Claim 35, wherein the data storage deletes the second storage key depending upon whether the third storage key is stored into the second content storing means.

37. The system as set forth in Claim 36, wherein the key management unit comprises means for storing the second storage key and the identification information of the second content storing means in which the content key encrypted with the second storage key is stored; the key management unit accounts, when the data storage decrypts the content key, the data service following the predetermined procedure based on the result of comparison between the identification information of the second content storing means, sent from the data storage, and the identification information stored in the identification information storing means.

38. The system as set forth in Claim 31, wherein the second content storing means has stored therein the identification information of the data storage.

39. The system as set forth in Claim 38, wherein the data storage starts decrypting the content key stored in the second content storing means.

40. The system as set forth in Claim 20, wherein the content key obtained by decryption from the second content storing means has added thereto information that the content key is a one obtained by restoration, as requirement information.

41. The system as set forth in Claim 20, wherein the content key has added thereto frequency information which limits the number of times the content key can be used.